October 2023

TechTidbit.com

brought to you by Tech Experts

# Cybersecurity Skeletons In Your Business' Closet

*Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.*

Let's dive into a topic that might give you the chills - cybersecurity skeletons in your company's closet.

You may not have old skeletons hidden away in the basement, but there's a good chance of cybersecurity vulnerabilities lurking in the shadows. Just waiting to wreak havoc.

You can't fix what you can't see. It's time to shine a light on these hidden dangers, so you can take action to protect your business from potential cyber threats.

Here are some of the most common cybersecurity issues faced by small and mid-sized businesses:

## Outdated software: The cobweb-covered nightmare

Running outdated software is like inviting hackers to your virtual Halloween party.

When software vendors release updates, they often include crucial security patches. These patches fix vulnerabilities that hackers can exploit. Keep everything up to date to ensure your digital fortress is secure.

## Weak passwords: The skeleton key for cybercriminals

If your passwords are weak, you might as well be handing out your office keys to cybercriminals.

Instead, create strong and unique passwords for all accounts and devices. Consider using a mix of upper and lowercase letters, numbers, and special characters.

## Unsecured Wi-Fi: The ghostly gateway

Ensure your Wi-Fi is password-protected. Make sure your router uses WPA2 or WPA3 encryption for an added layer of security. For critical business tasks, consider a virtual private network (VPN). It can shield your data from prying eyes.

## Lack of training: The haunting ignorance

Employee error is the cause of approximately 88% of all data breaches.

Without proper cybersecurity training, your staff might unknowingly fall victim to phishing scams. Or inadvertently expose sensitive information. Regularly educate your team about cybersecurity best practices, such as:

- Recognizing phishing emails
- Avoiding suspicious websites
- Using secure file-sharing methods

## No data backups: The cryptic catastrophe

Imagine waking up to find your business's data gone, vanished into the digital abyss. Without backups, this nightmare can become a reality.

Embrace the 3-2-1 rule. Have at least three copies of your data stored on two different media types. With one copy stored securely offsite.

## No MFA: The ghoulish gamble

Adding multi-factor authentication (MFA) provides an extra layer of protection. It requires users to provide extra authentication factors, such as a one-time code sent by email or text, or passkey. This makes it much harder for cyber attackers to breach your accounts.

## Ignoring mobile security: The haunted phones

Ensure that all company-issued devices have passcodes or biometric locks enabled. Consider implementing mobile device management (MDM) solutions.

These will enable you to enforce security policies.

## Shadow IT: The spooky surprise

Shadow IT refers to the use of unauthorized applications within your business. It might seem harmless when employees use convenient tools they find online.

Regularly audit your systems to uncover any shadow IT lurking under cover.

When software vendors release updates, they often include crucial security patches. These patches fix vulnerabilities that hackers can exploit. Keep everything up to date to ensure your digital fortress is secure.

# What is SaaS Ransomware? How Can You Defend Against It?

*"Frequently backing up your SaaS data is crucial. Having up-to-date backups ensures that you can restore your files. You won't need to pay the attacker's ransom demands and you'll get your business back up and running faster."*


Software-as-a-Service (SaaS) has revolutionized the way businesses operate. But alongside its benefits, SaaS brings with it potential threats. When software and data are online, they're more vulnerable to attacks. One of the latest threats to move from endpoint devices to the cloud is ransomware.

Between March and May of 2023, SaaS attacks increased by over 300%. A study in 2022 by Odaseva found that 51% of ransomware attacks targeted SaaS data.

## What is SaaS ransomware?

SaaS ransomware is also known as cloud ransomware. It's malicious code designed to target cloud-based applications and services. These include services like Google Workspace, Microsoft 365, and other cloud collaboration platforms. Here are some tips to defend your business from SaaS ransomware.

## Educate your team

Start by educating your employees about the risks of SaaS ransomware. Include how it spreads through phishing emails, malicious links, or breached accounts. Teach them to recognize suspicious activities and report any unusual incidents immediately.

## Enable multi-factor authentication (MFA)

MFA is an essential layer of security. Enabling MFA reduces the risk of unauthorized access. This is true, even if a hacker compromises an account's login credentials.

## Regular backups

Frequently backing up your SaaS data is crucial. Having up-to-date backups ensures that you can restore your files. You won't need to pay the attacker's ransom demands and you'll get your business back up and running faster.

## Deploy advanced security solutions

Consider using third-party security solutions that specialize in protecting SaaS environments.

These solutions can provide many benefits including:

- Real-time threat detection
- Data loss prevention
- And other advanced security features

## Apply the principle of least privilege

Limit user permissions to only the necessary functions. By doing this, you reduce the potential damage an attacker can do if they gain access.

## Keep software up to date

Ensure that you keep all software up to date. Regular updates close known vulnerabilities and strengthen your defense.

## Track suspicious account activity

Put in place robust monitoring of user activity and network traffic. Suspicious behavior can be early indicators of an attack. One example to watch for is several failed login attempts. Another is access from unusual locations.

## Develop an incident response plan

Prepare and practice an incident response plan. It should outline the steps to take in the event of a ransomware attack. A well-coordinated response can mitigate the impact of an incident. It can also aid in faster recovery. The sooner your team can respond, the faster business gets back to normal.

**Did you know? You can create new service requests, check ticket status, and review invoices in our client portal. Browse to: *http://www.TechSupportRequest.com***

# Collaboration Tools Are GREAT. But Are They A Security Risk?

In today's digital age, workplace collaboration tools and messaging apps such as Slack, Teams, and Zoom have become indispensable.

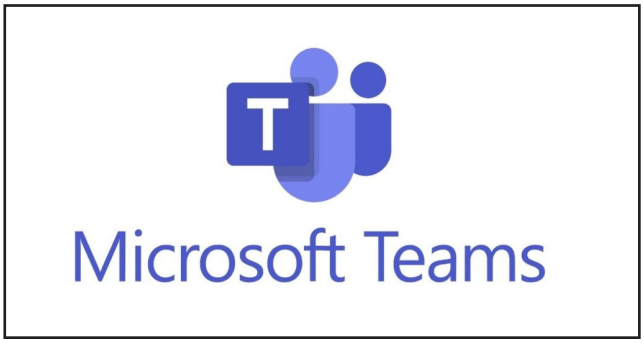
They've revolutionized the way we work, making communication with colleagues a breeze, facilitating seamless file sharing, and allowing for productive meetings without the hassle of commuting.

The ability to discuss even the most sensitive of topics from the warmth and safety of our homes seems like a dream. However, every silver lining has a cloud.

While we see these tools as productivity enhancers, cybercriminals see them as gateways to potential vulnerabilities. The very platforms that have been champions for our productivity are simultaneously creating a playground for cyber threats.

It's alarming to realize that, for instance, while Slack employs encryption, it does not have end-to-end encryption. The reason behind this? To provide companies with an overview of their internal communications.

Moreover, if you've jumped on the WhatsApp bandwagon for business, beware. This popular app has been a victim of numerous social engineering attacks. And Telegram? It's steadily climbing the list of hotspots for cyber attackers.




These threats have ushered in a new form of cyber-attack known as Business Communication Compromise (BCC).

Think of it as the menacing relative of the widely recognized Business Email Compromise (BEC).

Shockingly, a 2022 Data Breach Investigation Report highlighted that a staggering 82% of data breaches stem from human errors. Just one misguided click on a deceitful phishing email, and your prized communication channels become a hotbed for these cyber rogues.

But there's hope! Here are some measures to safeguard your digital spaces:

• **Establish robust access controls.** Ensure that only authorized individuals can access your platform. Even basic protocols like multi-factor authentication can act as formidable barriers against intruders.

• **Adopt stringent data loss prevention techniques.** Opt for systems that provide end-to-end encryption and have capabilities to remotely wipe data from misplaced or stolen devices.

• **Educate your team.** Regular training sessions on best practices for handling sensitive information can make all the difference.

Your security is our priority. If you need guidance on fortifying your digital defenses, we're here to assist.

*"While we see these tools as productivity enhancers, cybercriminals see them as gateways to potential vulnerabilities. The very platforms that have been champions for our productivity are simultaneously creating a playground for cyber threats."*

## We Love Referrals!

The greatest gift anyone can give us is a referral to your friends and business colleagues. Referrals help us keep costs down so we can pass the savings to our clients.

If your friend ends up becoming a client - we'll give them their free first month of service (for being a friend of yours) AND we'll give you a $250 Amazon Gift Card.

Simply introduce us via email to sales@mytechexperts.com and we'll take it from there. We'll look after your friend's business with a high level of care and attention (just like we do with all our clients).

**Contact Information**

**Tech Experts Support Team**
(734) 240-0200
support@MyTechExperts.com

**Main Office**
(734) 457-5000
info@MyTechExperts.com

**Sales Inquiries**
(888) 457-5001
sales@MyTechExperts.com

TECH EXPERTS

**15347 South Dixie Highway**
**Monroe, MI 48161**
**Tel (734) 457-5000**
**Fax (734) 457-4332**
**info@MyTechExperts.com**



# Is AI Really For You, Or Are You Jumping On The Bandwagon?

Do you ever find yourself asking, "What is all this hype about AI?"

If so, you're not alone.

The buzz around artificial intelligence (AI) and its potential to revolutionize every aspect of our lives is inescapable. But how can you navigate through the noise and truly harness the power of AI to meet your business's big goals?

It's a question that keeps many business leaders awake at night.

Imagine being able to predict market trends before they happen, or to streamline your operations with almost exact precision. This isn't some far-off dream; it's the promise of generative AI.

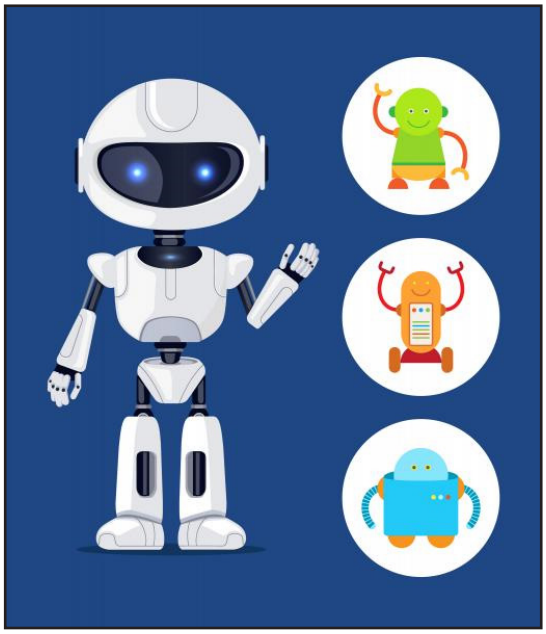
But there's a lot of speculation around AI. Right now, it's uncertain, so… should you simply wait and see what happens?

Of course not!

In fact, now is exactly the time to start exploring generative AI for your company.

Sitting back isn't an option when your rivals could be leveraging this technology to gain a competitive edge. Yes, there's a lot to learn and understand, but isn't that part of the thrill of doing business in the 21st century?

But one thing to keep in mind amidst the excitement, is not to lose sight of your core aims, goals, and cultures. What good is a new AI system if it doesn't align with the way your business behaves?



While the world of AI may seem like uncharted territory, some classic rules still apply.

Will you implement it? Will it generate revenue? Can it reduce your costs? Will it boost productivity? If not, perhaps it's not the right move for your business right now.

## The hackers are using AI, too

With the advancement of AI comes new developments for bad actors to weaponize, too.

Artificial intelligence has become incredibly powerful. We can create animated avatars of ourselves with just a facial scan. A few words in the right search engine can generate beautiful imagery and art.

You can even find AI to write entire book chapters (although, they don't always make much sense).

Unfortunately, cybercriminals have learned how to code entirely new malware in significantly less time than it takes to build by hand.

Usually, malware takes up to an hour to code. Not ChatGPT: the chatbot can code phishing scams honed to lure in more victims, and it can do it in mere minutes.

It also creates infected attachments that try to give the hacker remote access to your machine. Hackers will be able to really hone their scam messages using AI that has quantitative knowledge about what works best.

They can fine-tune their ability to detect exploitable vulnerabilities on your systems. Who knows what threatening idea they'll have artificial intelligence machines make a reality for them next?

Users need to be careful engaging with nascent technology and stay abreast of new developments that the good guys are working on, so that we can all stay ahead of cybercriminals no matter what they dream up next.